

# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0826U002033

**Особливі позначки:** відкрита

**Дата реєстрації:** 29-05-2026

**Статус:** Наказ про видачу диплома

**Реквізити наказу МОН / наказу закладу:**



## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Наumenко Сергій Васильович

2. Serhii V. Naumenko

**Кваліфікація:**

**Ідентифікатор ORCID ID:** 0000-0002-6337-1605

**Вид дисертації:** доктор філософії

**Аспірантура/Докторантура:** так

**Шифр наукової спеціальності:** 123

**Назва наукової спеціальності:** Комп'ютерна інженерія

**Галузь / галузі знань:** інформаційні технології

**Освітньо-наукова програма зі спеціальності:** Комп'ютерні системи та мережі

**Дата захисту:** 05-06-2026

**Спеціальність за освітою:** Системне програмування

**Місце роботи здобувача:** Черкаський національний університет імені Богдана Хмельницького

**Код за ЄДРПОУ:** 02125622

**Місцезнаходження:** бульвар Шевченка, Черкаси, Черкаський р-н., 18031, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

### **III. Відомості про організацію, де відбувся захист**

**Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради):** PhD 13027

**Повне найменування юридичної особи:** Черкаський державний технологічний університет

**Код за ЄДРПОУ:** 05390336

**Місцезнаходження:** бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

### **IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію**

**Повне найменування юридичної особи:** Черкаський державний технологічний університет

**Код за ЄДРПОУ:** 05390336

**Місцезнаходження:** бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

### **V. Відомості про дисертацію**

**Мова дисертації:** Українська

**Коди тематичних рубрик:** 20.54, 20.55, 20.56

**Тема дисертації:**

1. Метод та моделі захисту інформації для кіберфізичних систем з обмеженими ресурсами.
2. Information protection method and models for cyber-physical systems with limited resources.

**Реферат/анотація:**

1. Дисертаційна робота присвячена підвищенню рівня криптографічного захисту інформації в кіберфізичних системах (КФС), що функціонують в умовах обмежених обчислювальних ресурсів, енергоспоживання та жорстких часових обмежень. Проведено аналіз архітектурних рівнів КФС, класифікацію загроз інформаційній безпеці та обґрунтовано доцільність застосування полегшених криптографічних механізмів. Розроблено модель захисту на рівні сенсорних вузлів і вбудованих пристроїв із підтримкою Secure Boot та управління ключовим матеріалом. Побудовано моделі захищеного обміну даними в мережевих та edge-архітектурах. Запропоновано метод побудови комплексної системи криптографічного захисту з адаптивним вибором алгоритмів залежно від ресурсних можливостей компонентів. Метод реалізовано на мікроконтролері STM32 у середовищах FreeRTOS та bare-metal. Експериментально підтверджено зниження енергоспоживання на 23%, обчислювального навантаження на 35–40% та підвищення продуктивності на 20–25% порівняно з традиційними підходами.

2. The dissertation addresses the problem of enhancing cryptographic information protection in cyber-physical systems (CPS) operating under constraints of limited computational resources, energy consumption, and strict timing requirements. The study analyzes the architectural layers of CPS, classifies information security threats, and justifies the use of lightweight cryptographic mechanisms. A protection model for sensor nodes and embedded devices is developed, incorporating Secure Boot and key material management. Models for secure data exchange in network and edge architectures are constructed. A method for building a comprehensive cryptographic protection system with adaptive algorithm selection based on component resource capabilities is proposed. The method is implemented on an STM32 microcontroller under FreeRTOS and bare-metal environments. Experimental results confirm a 23% reduction in energy consumption, a 35–40% decrease in computational load, and a 20–25% improvement in system performance compared to conventional approaches.

**Державний реєстраційний номер ДіР:**

**Пріоритетний напрям розвитку науки і техніки:** Інформаційні та комунікаційні технології

**Стратегічний пріоритетний напрям інноваційної діяльності:** Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

**Підсумки дослідження:** Нове вирішення актуального наукового завдання

**Публікації:**

- Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography. Proceedings of the 6th International Conference on Informatics & Data-Driven Medicine (IDDM'2023). 2023. P. 145–146. URL: <https://ceur-ws.org/Vol-3609/paper12.pdf>
- Rozlomii I., Yarmilko A., Naumenko S. Data security of IoT devices with limited resources: challenges and potential solutions. Proceedings of the 4th Edge Computing Workshop (DOORS 2024). 2024. Vol. 3666. P. 85–96. URL: <https://ceurws.org/Vol-3666/paper13.pdf>
- Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. The role of encryption in information protection for cloud computing. IEEE 4th International Conference on Smart Information Systems and Technologies (SIST). 2024. P. 70–75. URL: <https://doi.org/10.1109/SIST61555.2024.10629501>
- Yarmilko A., Rozlomii I., Naumenko S. Dependability of embedded systems in the Industrial Internet of Things: Information security and reliability of the communication cluster. Information Technology for Education, Science, and Technics. 2024. Vol. 222. P. 235–249. URL: [https://doi.org/10.1007/978-3-031-71804-5\\_16](https://doi.org/10.1007/978-3-031-71804-5_16)
- Rozlomii I., Naumenko S., Mykhailovskyi P., Monarkh V. Resourcesaving cryptography for microcontrollers in biomedical devices. IEEE 5th KhPI Week on Advanced Technology (KhPIWeek). 2024. P. 1–5. URL: <https://doi.org/10.1109/KhPIWeek61434.2024.10877958>
- Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. Hardware encryptors and cryptographic libraries for optimizing security in IoT. Proceedings of the 12th International Conference Information Control Systems & Technologies (ICST 2024). 2024. Vol. 3790. P. 99–109. URL: <https://ceur-ws.org/Vol-3790/paper09.pdf>
- Rozlomii I., Yarmilko A., Naumenko S. Security and efficiency models for cyber-physical systems in medical devices. IEEE 19th International Conference on Computer Science and Information Technologies (CSIT). 2024. P. 1–4. URL: <https://doi.org/10.1109/CSIT65290.2024.10982678>
- Rozlomii I., Yarmilko A., Naumenko S. Innovative resource-saving security strategies for IoT devices. Journal of Edge Computing. 2025. Vol. 4, no. 1. P. 35–56. URL: <https://doi.org/10.55056/jec.748>
- Rozlomii I., Yarmilko A., Naumenko S. Vulnerability modeling in cybersecurity of intelligent infrastructure networks. International Scientific-Practical Conference. 2024. P. 234–248. URL: [https://doi.org/10.1007/978-3-031-90735-7\\_19](https://doi.org/10.1007/978-3-031-90735-7_19)
- Rozlomii I., Yarmilko A., Naumenko S. Resource-efficient solutions for data security at the network level of the Medical Internet of Things. Proceedings of the 7th International Conference on Informatics & Data-

Driven Medicine (IDDM'2024). 2024. P. 171–182. URL: <https://ceur-ws.org/Vol-3892/paper13.pdf>

- Faure E., Rozlomii I., Yarmilko A., Naumenko S. Protection of IoT networks: cryptographic solutions for cybersecurity management. Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024). 2024. P. 24–34. URL: <https://ceurws.org/Vol-3925/paper03.pdf>
- Rozlomii I., Yarmilko A., Naumenko S. Integration of lightweight cryptography and artificial intelligence methods to increase the dependability of precision medicine systems. Proceedings of the International Workshop on Computational Intelligence (IWSCI 2025), co-located with the IV International Scientific Symposium “Intelligent Solutions” (IntSol 2025), Kyiv–Uzhhorod, May 01– 05, 2025. 2025. P. 201–212. URL: <https://ceur-ws.org/Vol-4035/Paper17.pdf>
- Faure E., Rozlomii I., Naumenko S. Cryptographic load sharing method in critical infrastructure sensor networks. Proceedings of the Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN-25). 2025. P. 24–34. URL: <https://ceur-ws.org/Vol-4024/paper01.pdf>
- Rozlomii I., Naumenko S., Mykhailovskyi P., Lishchuk R. Methodology for selecting the protection strategy in IoT environments based on the device resource profile. IEEE 6th KhPI Week on Advanced Technology (KhPIWeek). 2025. P. 1–5. URL: <https://doi.org/10.1109/KhPIWeek61436.2025.11288556>
- Danchenko O., Rozlomii I., Yarmilko A., Naumenko S. A lightweight Secure Boot mechanism for protecting the firmware of IoT devices. Proceedings of the 13-th International Conference Information Control Systems & Technologies (ICST 2025), Odesa, Ukraine, September 24–26, 2025. CEUR Workshop Proceedings, Vol. 4048. 2025. P. 240–250. URL: <https://ceur-ws.org/Vol-4048/paper19.pdf>
- Rozlomii I., Faure E., Yarmilko A., Naumenko S. The method for verifying firmware integrity in IoT devices for secure boot using lightweight hash functions. Proceedings of the Cyber Security and Data Protection (CSDP 2025), Lviv, Ukraine, July 31, 2025. CEUR Workshop Proceedings, Vol. 4042. 2025. P. 105–116. URL: <https://ceur-ws.org/Vol-4042/paper8.pdf>
- Rozlomii I., Naumenko S., Trembovetskyi R. Method for rotating cryptographic keys based on time tokens for radio-electronic medical modules with limited resources. Visnyk NTUU KPI Serii Radiotekhnika Radioaparotobuduvannia. 2025. No. 102. P. 58–65. URL: <https://doi.org/10.64915/RADAP.2025.102.58-65>
- Zabolotnii S., Rozlomii I., Yarmilko A., Naumenko S. Reconfigured CoARX architecture for implementing ARX hashing in microcontrollers of IoT systems with limited resources. Informatyka, Automatyka, Pomiar w Gospodarce i Ochronie Środowiska. 2025. Vol. 15, no. 4. P. 164–169. URL: <https://doi.org/10.35784/iapgos.7782>
- Faure E., Rozlomii I., Naumenko S. Hybrid digital twin-driven anomaly detection in IoT telemetry using LSTM autoencoder. Proceedings of the 2nd International Workshop on Data Analytics (WDA 2026), Kyiv, Ukraine, January 26, 2026. CEUR Workshop Proceedings, Vol. 4155. 2025. P. 76–89. URL: <https://ceurws.org/Vol-4155/paper06.pdf>
- Розломій І. О., Косенюк Г. В., Науменко С. В., Михайловський П. В. Моделювання системи датчиків на базі мікроконтролера в ігровій симуляції «Смарт-будинки» з використанням шифрування. Computer-Integrated Technologies: Education, Science, Production. 2023. Вип. 53. С. 292–299. URL: <https://doi.org/10.36910/6775-2524-0560-2023-53-43>
- Розломій І. О., Симонюк В. П., Науменко С. В., Михайловський П. В. Адаптивна криптографія для енергоефективного захисту пристроїв IoT. Проблеми моделювання та автоматизації проектування. 2024. № 1(19). С. 77– 83. URL: <https://doi.org/10.31474/2074-7888-2024-1-19-77-83>
- Розломій І. О., Симонюк В. П., Науменко С. В., Михайловський П. В. Модель безпеки взаємопов'язаних обчислювальних пристроїв на основі полегшеної схеми шифрування для IoT. Computer-Integrated Technologies: Education, Science, Production. 2024. Вип. 55. С. 191–198. URL: <https://doi.org/10.36910/6775-2524-0560-2024-55-24>

- Rozlomii O., Yarmilko A., Naumenko S. The intelligent approaches to organizing secure information exchange in dynamic swarms of unmanned platforms. *Artificial Intelligence*. 2024. Vol. 29, no. 4. P. 151–158. URL: <https://doi.org/10.15407/jai2024.04.151>
- Розломій І. О., Науменко С. В. Моделювання взаємовпливу інформаційної безпеки та обчислювальних витрат у вбудованих пристроях. *Computer-Integrated Technologies: Education, Science, Production*. 2024. Вип. 57. С. 139–145. URL: <https://doi.org/10.36910/6775-2524-0560-2024-57-16>
- Розломій І. О., Фауре Е. В., Науменко С. В. Методи аутентифікації у вбудованих системах з обмеженими обчислювальними ресурсами. Вимірювальна та обчислювальна техніка в технологічних процесах. 2025. Вип. 81. С. 29–35. URL: <https://doi.org/10.31891/2219-9365-2025-81-4>
- Розломій І. О., Науменко С. В. Архітектура та функціональні особливості захищених систем керування базами даних нового покоління з підтримкою serverless та edge-обчислень. *Systems and Technologies*. 2025. №1 (69), С. 7–15. URL: <https://doi.org/10.32782/2521-6643-2025-1-69.16>
- Розломій І. О., Науменко С. В., Симонюк В. В., Птащенко В. О., Зажом В. В. Полегшена криптографія для безпеки параметрів вібрації в постобробці 3D-друкованих деталей. *Інформаційні технології та суспільство*. 2025. № 2(17). С. 175–182. URL: <https://doi.org/10.32689/maup.it.2025.2.25>
- Rozlomii I., Koseniuk G., Naumenko S. Mechanisms for cryptographic code authentication control in sensor nodes with limited computing resources. *Computer-Integrated Technologies: Education, Science, Production*. 2025. No. 61. P. 193–198. URL: <https://doi.org/10.36910/6775-2524-0560-2025-61-27>
- Розломій І., Науменко С., Ковтюх В. Модель захищеного зберігання даних у розподілених базах даних на основі атрибутного шифрування для критичних інформаційно-комунікаційних систем. *Measuring and Computing Devices in Technological Processes*. 2026. № 1. С. 215–220. URL: <https://doi.org/10.31891/2219-9365-2026-85-27>
- Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. Modern encryption methods in IoT: hardware solutions and cryptographic libraries for data. *Розвитки інформаційно-керуючих систем та технологій: монографія / за ред. В. Вичужаніна. Львів-Торунь: Liha-Pres, 2024. P. 28–44. URL: <https://doi.org/10.36059/978-966-397-422-4>*
- Розломій І. О., Ярмілко А. В., Науменко С. В. Ресурсоощадний підхід до побудови secure boot у вбудованих системах інтернету речей. Системи контролю інформації та інтелектуальні технології. Досягнення та застосування: монографія / за ред. В. Вичужаніна. Львів-Торунь: Liha-Pres, 2025. С. 102–122. URL: <https://doi.org/10.36059/978-966-397-538-2-6>
- Rozlomii I., Yarmilko A., Naumenko S. Towards distributed anomaly detection in smart networks: a power-efficient node-level approach. *Методи та засоби обчислювального інтелекту в управлінні смарт-системами: колективна монографія / за ред. В. М. Теслюка. Львів, 2025. С. 109–118.*
- Yarmilko A., Rozlomii I., Naumenko S. Robust communication clusters: Secure information exchange and redundant hashing for third-party inclusions localization. *КЗЯТПС-2023: тези доп. Чернівці, 2023. P. 224–225.*
- Науменко С. В., Розломій І. О. Information protection strategies in Industry 4.0: Encryption and cybersecurity for industrial systems. *Theoretical and Experimental Research in Materials Science and Mechanical Engineering: матеріали IX Міжнар. наук.-практ. конф., Луцьк, 2023. Луцьк: Вежа-Друк, 2023. С. 191–193.*
- Науменко С. В., Розломій І. О., Михайловський П. В. Забезпечення кібербезпеки в Smart-імплантах: роль полегшеної криптографії. *Інформаційна безпека та комп'ютерні технології: матеріали VII Міжнар. наук.-практ. конф., м. Кропивницький, 1 листоп. 2023 р. Кропивницький, 2023. С. 17–18.*
- Rozlomii I. O., Yarmilko A., Naumenko S. Optimized hash functions for integrity control and data recovery in embedded systems. *Information-Management Systems and Technologies: матеріали XI Міжнар. наук. конф. 2023. С. 31–34.*
- Rozlomii I., Yarmilko A., Naumenko S., Mykhailovskyi P. The comprehensive IoT security strategy using hardware and software encryption methods. *Information-Management Systems and Technologies: матеріали*

XII Міжнар. наук. конф., Одеса, 23 – 25 верес. 2024 р. Одеса, 2024. С. 63–65.

- Розломій І. О., Ярмілко А. В., Науменко С. В. Інтелектуальні підходи до організації інформаційного обміну в динамічних зграях безпілотних платформ. Штучний інтелект та інтелектуальні системи (AHS'2024): матеріали XXIV Міжнар. наук.-техн. конф. 2024. С. 144–149.
- Науменко С. В., Михайловський П. В., Стабецька Т. А. Сучасні технології захисту даних у вбудованих пристроях з обмеженими ресурсами. Free and Open Source Software: матеріали Міжнар. наук.-практ. конф., Харків, 13 – 14 лют. 2025 р. Харків, 2025. С. 63–64.
- Розломій І. О., Науменко С. В. Конфігурований ARX-примітив для енергоефективного хешування у пристроях IoT. Інформаційні системи та технології: результати і перспективи (IST 2025): матеріали II Міжнар. наук.-практ. конф. 2025. С. 269–271.
- Чікін Д. М., Науменко С. В., Розломій І. О. Захист персональних даних в IoT-пристроях із застосуванням штучного інтелекту. Інформаційна безпека та комп'ютерні технології: тези доп. VIII Міжнар. наук.-практ. конф., м. Кропивницький, 24 – 25 квіт. 2025 р. Кропивницький: ЦНТУ, 2025. С. 12–13.
- Розломій І. О., Науменко С. В., Михайловський П. В. Формування сеансових ключів у сенсорних пристроях з обмеженим обсягом пам'яті на основі часових токенів. Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2025): матеріали XV Міжнар. наук.-практ. конф., Чернігів, 22 – 23 трав. 2025 р. Чернігів: НУ «Чернігівська політехніка», 2025. Вип. 2. С. 248–249.
- Розломій І. О., Науменко С. В. Метод розподілу криптографічного навантаження між мікроконтролерами в edge-архітектурах на основі енергетичної моделі. Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем: матеріали II Міжнар. наук.-практ. конф., Луцьк, 2025. Луцьк: ЛНТУ, 2025. С. 112–115.
- Розломій І. О., Науменко С. В. Модель адаптивної побудови довірчих IoT-мереж із динамічною ротацією вузлів. Програмне та апаратне забезпечення в інформаційних технологіях: матеріали Міжнар. наук.-практ. конф. молодих вчених та студентів, Луцьк, 6 трав. 2025 р. / відп. ред. Т. В. Терлецький. Луцьк: ЛНТУ, 2025. Вип. 1. С. 136–139.

**Наукова (науково-технічна) продукція:** методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація

**Соціально-економічна спрямованість:** підвищення автоматизації виробничих процесів; забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

**Охоронні документи на ОПІВ:**

**Впровадження результатів дисертації:** Планується до впровадження

**Зв'язок з науковими темами:**

## **VI. Відомості про наукового керівника/керівників (консультанта)**

**Власне Прізвище Ім'я По-батькові:**

1. Розломій Інна Олександрівна

2. Inna O. Rozlomii

**Кваліфікація:** к. т. н., 05.13.05

**Ідентифікатор ORCID ID:** 0000-0001-5065-9004

**Додаткова інформація:** ;<https://orcid.org/0000-0001-5065-9004>;<https://scholar.google.com.ua/citations?user=N7AnL5YAAAAJ&hl=ru>

**Повне найменування юридичної особи:** Черкаський національний університет імені Богдана Хмельницького

**Код за ЄДРПОУ:** 02125622

**Місцезнаходження:** бульвар Шевченка, Черкаси, Черкаський р-н., 18031, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

## **VII. Відомості про офіційних опонентів та рецензентів**

### **Офіційні опоненти**

#### **Власне Прізвище Ім'я По-батькові:**

1. Смірнова Тетяна Віталіївна

2. Tetiana V. Smirnova

**Кваліфікація:** к. т. н., доц., 05.02.01

**Ідентифікатор ORCID ID:** 0000-0001-6896-0612

#### **Додаткова інформація:**

**Повне найменування юридичної особи:** Центральноукраїнський національний технічний університет

**Код за ЄДРПОУ:** 0205070950

**Місцезнаходження:** просп. Університетський, Кропивницький, Кропивницький р-н., 25030, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

#### **Власне Прізвище Ім'я По-батькові:**

1. Поліщук Микола Миколайович

2. Mukola Polishchuk

**Кваліфікація:** к. т. н., доц., 05.05.11

**Ідентифікатор ORCID ID:** 0000-0002-1218-5925

#### **Додаткова інформація:**

**Повне найменування юридичної особи:** Луцький національний технічний університет

**Код за ЄДРПОУ:** 05477296

**Місцезнаходження:** вул. Львівська, Луцьк, Луцький р-н., 43018, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** 02vn54r74

## **Рецензенти**

### **Власне Прізвище Ім'я По-батькові:**

1. Лавданський Артем Олександрович
2. Artem O. Lavdanskyi

**Кваліфікація:** к. т. н., доц., 05.13.05

**Ідентифікатор ORCID ID:** 0000-0002-1596-4123

### **Додаткова інформація:**

**Повне найменування юридичної особи:** Черкаський державний технологічний університет

**Код за ЄДРПОУ:** 05390336

**Місцезнаходження:** бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

### **Власне Прізвище Ім'я По-батькові:**

1. Чепинога Анатолій Володимирович
2. Anatolii V. Cherynoga

**Кваліфікація:** к. т. н., доц., 01.05.02

**Ідентифікатор ORCID ID:** 0000-0003-3921-6557

### **Додаткова інформація:**

**Повне найменування юридичної особи:** Черкаський державний технологічний університет

**Код за ЄДРПОУ:** 05390336

**Місцезнаходження:** бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

## **VIII. Заключні відомості**

**Власне Прізвище Ім'я По-батькові**  
**голови ради**

Бабенко Віра Григорівна

**Власне Прізвище Ім'я По-батькові**  
**головуючого на засіданні**

Бабенко Віра Григорівна

**Відповідальний за підготовку  
облікових документів**

Здобувач PhD

**Реєстратор**

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є  
відповідальним за реєстрацію наукової  
діяльності**



Юрченко Тетяна Анатоліївна